Configuring First Hop Redundancy Protocols in IPv6

Last Updated: December 5, 2011

IPv6 routing protocols ensure router-to-router resilience and failover. However, in situations in which the path between a host and the first-hop router fails, or the first-hop router itself fails, first hop redundancy protocols (FHRPs) ensure host-to-router resilience and failover.

The Gateway Load Balancing Protocol (GLBP) FHRP protects data traffic from a failed router or circuit, while allowing packet load sharing between a group of redundant routers. The Hot Standby Router Protocol (HSRP) protects data traffic in case of a gateway failure.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for First Hop Redundancy Protocols in IPv6

- Before configuring GLBP, ensure that the routers can support multiple MAC addresses on the physical interfaces. An additional MAC address is used for each GLBP forwarder to be configured.
- Avoid static link-local addressing on interfaces configured with GLBP.
- HSRP version 2 must be enabled on an interface before HSRP IPv6 can be configured.

Information About First Hop Redundancy Protocols in IPv6

GLBP for IPv6

GLBP for IPv6 Overview

The Gateway Load Balancing Protocol feature provides automatic router backup for IPv6 hosts configured with a single default gateway on an IEEE 802.3 LAN. Multiple first hop routers on the LAN combine to offer a single virtual first-hop IPv6 router while sharing the IPv6 packet forwarding load. GLBP performs a similar function for the user as HSRP. HSRP allows multiple routers to participate in a virtual router group configured with a virtual IPv6 address. One member is elected to be the active router to forward packets sent to the virtual IPv6 address for the group. The other routers in the group are redundant until the active router fails. These standby routers have unused bandwidth that the protocol is not using. Although multiple virtual router groups can be configured for the same set of routers, the hosts must be configured for different default gateways, which results in an extra administrative burden. The advantage of GLBP is that it additionally provides load balancing over multiple routers (gateways) using a single virtual IPv6 address and multiple virtual MAC addresses. The forwarding load is shared among all routers in a GLBP group rather than being handled by a single router while the other routers stand idle. Each host is configured with the same virtual IPv6 address, and all routers in the virtual router group participate in forwarding packets.

GLBP Benefits

GLBP for IPv6 provides the following benefits:

Load Sharing

You can configure GLBP in such a way that traffic from LAN clients can be shared equitably among multiple routers.

Multiple Virtual Routers

GLBP supports up to 1024 virtual routers (GLBP groups) on each physical interface of a router and up to four virtual forwarders per group.

Preemption

The redundancy scheme of GLBP enables you to preempt an active virtual gateway with a higher priority backup virtual gateway that has become available. Forwarder preemption works in a similar way, except that forwarder preemption uses weighting instead of priority and is enabled by default.

Authentication

You can also use the industry-standard Message Digest algorithm 5 (MD5) algorithm for improved reliability, security, and protection against GLBP-spoofing software. A router within a GLBP group with a different authentication string than other routers will be ignored by other group members. You can alternatively use a simple text password authentication scheme between GLBP group members to detect configuration errors.

GLBP Active Virtual Gateway

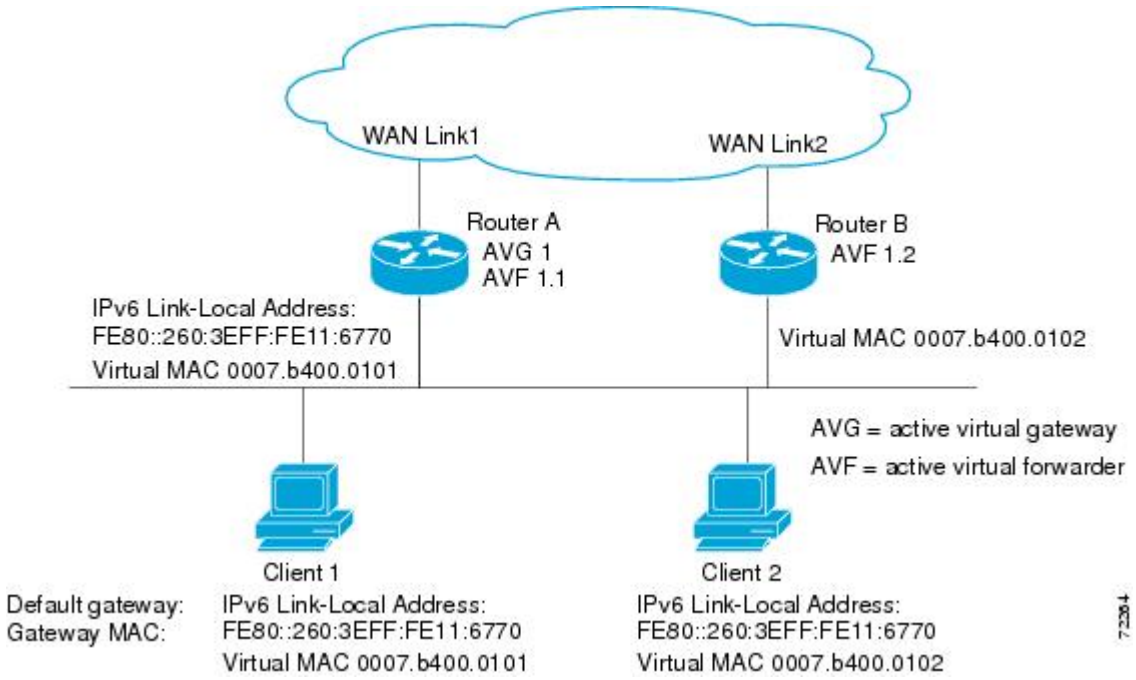
Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG in the event that the AVG becomes unavailable. The function of the AVG is that it assigns a virtual MAC address to each member of the GLBP group. Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as active virtual forwarders (AVFs) for their virtual MAC address.

The IPv6 neighbor discovery process uses Internet Control Message Protocol (ICMP) in IPv6 messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring routers. The IPv6 neighbor discovery process uses ICMPv6 messages and solicited-node multicast addresses to determine the link-layer address of a neighbor on the same network (local link), verify the reachability of a neighbor, and track neighboring routers. The AVG is responsible for answering ICMPv6 Neighbor Discovery requests for the virtual IPv6 address. Load sharing is achieved by the AVG replying to the ICMPv6 Neighbor Discovery requests with different virtual MAC addresses.

In the figure below, Router A is the AVG for a GLBP group, and is responsible for the IPv6 link-local address FE80::260:3EFF:FE11:6770. Router A is also an AVF for the virtual MAC address 0007.b400.0101. Router B is a member of the same GLBP group and is designated as the AVF for the virtual MAC address 0007.b400.0102. Client 1 has a default gateway IPv6 address of FE80::260:3EFF:FE11:6770 and a gateway MAC address of 0007.b400.0101. Client 2 shares the same

default gateway IP address but receives the gateway MAC address 0007.b400.0102 because Router B is sharing the traffic load with Router A.

Figure 1 GLBP Topology



If Router A becomes unavailable, Client 1 will not lose access to the WAN because Router B will assume responsibility for forwarding packets sent to the virtual MAC address of Router A, and for responding to packets sent to its own virtual MAC address. Router B will also assume the role of the AVG for the entire GLBP group. Communication for the GLBP members continues despite the failure of a router in the GLBP group.

GLBP Virtual MAC Address Assignment

A GLBP group allows up to four virtual MAC addresses per group. The AVG is responsible for assigning the virtual MAC addresses to each member of the group. Other group members request a virtual MAC address after they discover the AVG through hello messages. Gateways are assigned the next MAC address in sequence. A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. Other members of the GLBP group learn the virtual MAC addresses from hello messages. A virtual forwarder that has learned the virtual MAC address is referred to as a secondary virtual forwarder.

GLBP Virtual Gateway Redundancy

GLBP operates virtual gateway redundancy in the same way as HSRP. One gateway is elected as the AVG, another gateway is elected as the standby virtual gateway, and the remaining gateways are placed in a listen state.

If an AVG fails, the standby virtual gateway will assume responsibility for the virtual IPv6 address. A new standby virtual gateway is then elected from the gateways in the listen state.

GLBP Virtual Forwarder Redundancy

GLBP virtual forwarder redundancy is similar to virtual gateway redundancy with an AVF. If the AVF fails, one of the secondary virtual forwarders in the listen state assumes responsibility for the virtual MAC address.

The new AVF is also a primary virtual forwarder for a different forwarder number. GLBP migrates hosts away from the old forwarder number using two timers that start as soon as the gateway changes to the active virtual forwarder state. GLBP uses the hello messages to communicate the current state of the timers.

The redirect time is the interval during which the AVG continues to redirect hosts to the old virtual forwarder MAC address. When the redirect time expires, the AVG stops using the old virtual forwarder MAC address in ICMPv6 ND replies, although the virtual forwarder will continue to forward packets that were sent to the old virtual forwarder MAC address.

The secondary hold time is the interval during which the virtual forwarder is valid. When the secondary hold time expires, the virtual forwarder is removed from all gateways in the GLBP group. The expired virtual forwarder number becomes eligible for reassignment by the AVG.

GLBP Gateway Priority

GLBP gateway priority determines the role that each GLBP gateway plays and the results if the AVG fails.

Priority also determines if a GLBP router functions as a backup virtual gateway and the order of ascendancy to becoming an AVG if the current AVG fails. You can configure the priority of each backup virtual gateway with a value of 1 through 255 using the **glbp priority** command.

In the figure above, if Router A--the AVG in a LAN topology--fails, an election process takes place to determine which backup virtual gateway should take over. In this example, Router B is the only other member in the group so it will automatically become the new AVG. If another router existed in the same GLBP group with a higher priority, then the router with the higher priority would be elected. If both routers have the same priority, the backup virtual gateway with the higher IPv6 address would be elected to become the active virtual gateway.

By default, the GLBP virtual gateway preemptive scheme is disabled. A backup virtual gateway can become the AVG only if the current AVG fails, regardless of the priorities assigned to the virtual gateways. You can enable the GLBP virtual gateway preemptive scheme using the **glbp preempt** command. Preemption allows a backup virtual gateway to become the AVG, if the backup virtual gateway is assigned a higher priority than the current AVG.

GLBP Gateway Weighting and Tracking

GLBP uses a weighting scheme to determine the forwarding capacity of each router in the GLBP group. The weighting assigned to a router in the GLBP group can be used to determine whether it will forward packets and, if so, the proportion of hosts in the LAN for which it will forward packets. Thresholds can be set to disable forwarding when the weighting falls below a certain value. When the weighting rises above another threshold, forwarding is automatically reenabled.

The GLBP group weighting can be automatically adjusted by tracking the state of an interface within the router. If a tracked interface goes down, the GLBP group weighting is reduced by a specified value. Different interfaces can be tracked to decrement the GLBP weighting by varying amounts.

By default, the GLBP virtual forwarder preemptive scheme is enabled with a delay of 30 seconds. A backup virtual forwarder can become the AVF if the current AVF weighting falls below the low weighting threshold for 30 seconds. You can disable the GLBP forwarder preemptive scheme using the **no glbp**

forwarder preempt command or change the delay using the **glbp forwarder preempt delay minimum** command.

HSRP for IPv6

HSRP for IPv6 Overview

The HSRP is an FHRP designed to allow for transparent failover of the first-hop IP router. HSRP provides high network availability by providing first-hop routing redundancy for IP hosts on Ethernet configured with a default gateway IP address. HSRP is used in a group of routers for selecting an active router and a standby router. In a group of router interfaces, the active router is the router of choice for routing packets; the standby router is the router that takes over when the active router fails or when preset conditions are met.

IPv6 hosts learn of available IPv6 routers through IPv6 neighbor discovery RA messages. These are multicast periodically, or may be solicited by hosts. HSRP is designed to provide only a virtual first hop for IPv6 hosts.

An HSRP IPv6 group has a virtual MAC address that is derived from the HSRP group number, and a virtual IPv6 link-local address that is, by default, derived from the HSRP virtual MAC address. Periodic RAs are sent for the HSRP virtual IPv6 link-local address when the HSRP group is active. These RAs stop after a final RA is sent when the group leaves the active state.

Periodic RAs for the interface link-local address stop after a final RA is sent while at least one virtual IPv6 link-local address is configured on the interface. No restrictions occur for the interface IPv6 link-local address other than that mentioned for the RAs. Other protocols continue to receive and send packets to this address.

HSRP uses a priority mechanism to determine which HSRP configured router is to be the default active router. To configure a router as the active router, you assign it a priority that is higher than the priority of all the other HSRP-configured routers. The default priority is 100, so if you configure just one router to have a higher priority, that router will be the default active router.

HSRP IPv6 Virtual MAC Address Range

HSRP IPv6 uses a different virtual MAC address block than does HSRP for IP:

0005.73A0.0000 through 0005.73A0.0FFF (4096 addresses)

HSRP IPv6 UDP Port Number

Port number 2029 has been assigned to HSRP IPv6.

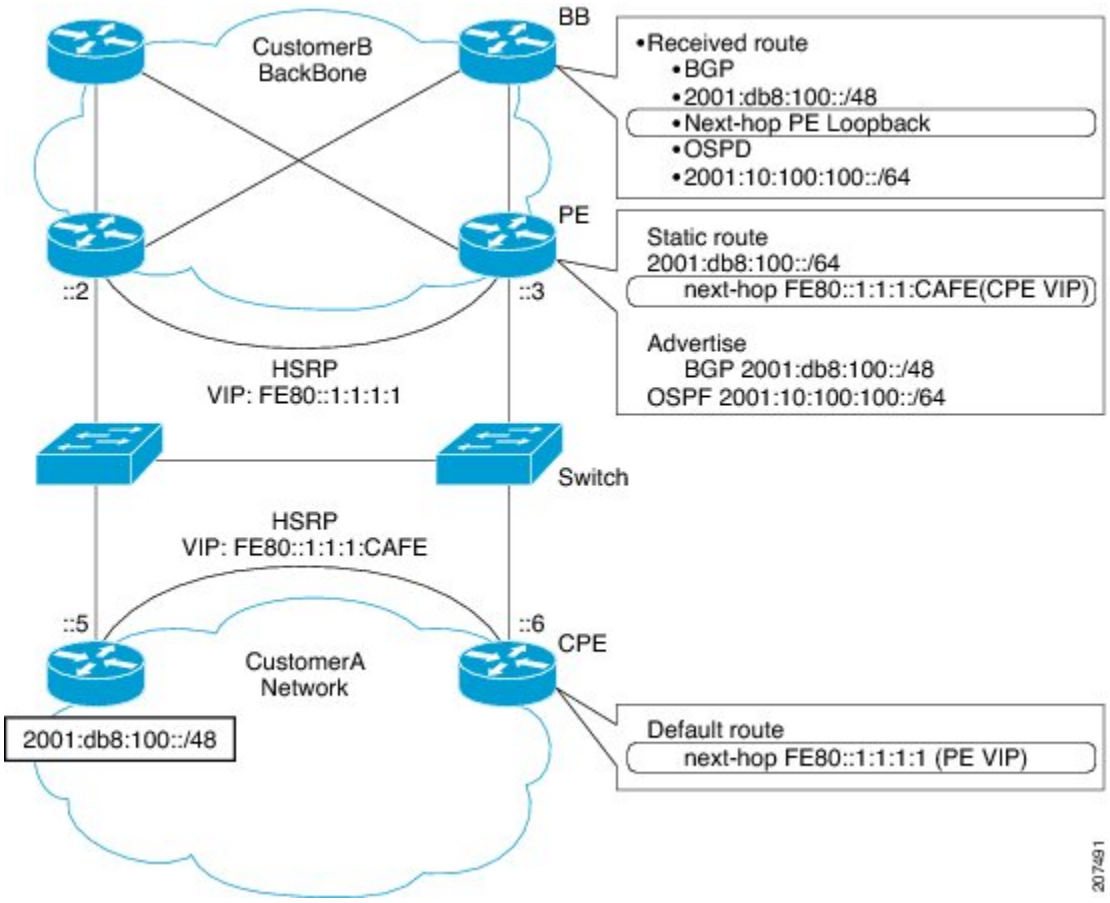
HSRP Global IPv6 Address

Note This feature is supported only in Cisco IOS Release 12.2(33)SXI4.

The HSRP global IPv6 address feature allows users to configure multiple nonlink local addresses as virtual addresses, and it allows for the storage and management of multiple global IPv6 virtual addresses in addition to the existing primary link-local address. If an IPv6 address is used, it must include an IPv6 prefix length. If a link-local address is used, it must not have a prefix.

The figure below depicts a deployment scenario that uses an HSRP IPv6 global virtual interface:

Figure 2 Scenario Using Gan HSRP IPv6 Global Virtual Interface



In the figure above, the provider equipment (PE) routers need to inject a route to reach the customer premises equipment (CPE) from the backbone routers. Because there are two CPEs, HSRP is convenient to use. The static route will be set with a link-local next hop (FE80::1:1:1:CAFE). If this address is injected in the backbone, this route is useless with a link-local next hop, as link-local addresses only have scope within the Layer 2 local LAN space. To address this issue, the next hop of the static route toward the virtual address must be set to a nonlink-local address, so backbone routers can route packets to the PE routers. At the next-hop address resolution, the active HSRP group member will reply to neighbor solicitation (NS) messages sent to the nonlink-local address.

How to Configure First Hop Redundancy Protocols in IPv6

Configuring and Customizing GLBP

Customizing GLBP behavior is optional. Be aware that as soon as you enable a GLBP group, that group is operating. It is possible that if you first enable a GLBP group before customizing GLBP, the router could take over control of the group and become the AVG before you have finished customizing the feature. Therefore, if you plan to customize GLBP, it is a good idea to do so before enabling GLBP.

This section contains the following optional procedures:

Customizing GLBP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** *ipv6-address / prefix-length | prefix-name ipv6-prefix / prefix-length* | **autoconfig** [*default-route*]}
5. **glbp** *group* **timers** [**msec**] *hellotime*[**msec**] *holdtime*
6. **glbp** *group* **timers redirect** *redirect timeout*
7. **glbp** *group* **load-balancing** [**host-dependent**| **round-robin**| **weighted**]
8. **glbp** *group* **priority** *level*
9. **glbp** *group* **preempt** [**delay minimum** *seconds*]
10. **glbp** *group* **name** *redundancy-name*
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address* / *prefix-length* | *prefix-name ipv6-prefix* / *prefix-length* | **autoconfig** [*default-route*]} **Example:** `Router(config-if)# ipv6 address 2001:DB8:0:7272::72/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 5	**glbp** *group* **timers** [**msec**] *hellotime*[**msec**] *holdtime* **Example:** `Router(config-if)# glbp 10 timers 5 18`	Configures the interval between successive hello packets sent by the AVG in a GLBP group. • The *holdtime* argument specifies the interval in seconds before the virtual gateway and virtual forwarder information in the hello packet is considered invalid. • The optional **msec** keyword specifies that the following argument will be expressed in milliseconds, instead of the default seconds.
Step 6	**glbp** *group* **timers redirect** *redirect timeout* **Example:** `Router(config-if)# glbp 10 timers redirect 600 7200`	Configures the time interval during which the AVG continues to redirect clients to an AVF. • The *timeout* argument specifies the interval in seconds before a secondary virtual forwarder becomes invalid.

	Command or Action	Purpose
Step 7	**glbp** *group* **load-balancing** [**host-dependent**| **round-robin**| **weighted**] **Example:** `Router(config-if)# glbp 10 load-balancing host-dependent`	Specifies the method of load balancing used by the GLBP AVG.
Step 8	**glbp** *group* **priority** *level* **Example:** `Router(config-if)# glbp 10 priority 254`	Sets the priority level of the gateway within a GLBP group. • The default value is 100.
Step 9	**glbp** *group* **preempt** [**delay minimum** *seconds*] **Example:** `Router(config-if)# glbp 10 preempt delay minimum 60`	Configures the router to take over as AVG for a GLBP group if it has a higher priority than the current AVG. • This command is disabled by default. • Use the optional **delay** and **minimum** keywords and the *seconds* argument to specify a minimum delay interval in seconds before preemption of the AVG takes place.
Step 10	**glbp** *group* **name** *redundancy-name* **Example:** `Router(config-if)# glbp 10 name abcompany`	Enables IPv6 redundancy by assigning a name to the GLBP group. • The GLBP redundancy client must be configured with the same GLBP group name so the redundancy client and the GLBP group can be connected.
Step 11	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns the router to global configuration mode.

Configuring GLBP Authentication

The following sections describe configuration tasks for GLBP authentication. The task you perform depends on whether you want to use text authentication, a simple MD5 key string, or MD5 key chains for authentication.

GLBP MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each GLBP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and, if the hash within the incoming packet does not match the generated hash, the packet is ignored.

The key for the MD5 hash can either be given directly in the configuration using a key string or supplied indirectly through a key chain.

A router will ignore incoming GLBP packets from routers that do not have the same authentication configuration for a GLBP group. GLBP has three authentication schemes:

- No authentication
- Plain text authentication
- MD5 authentication

GLBP packets will be rejected in any of the following cases:

- The authentication schemes differ on the router and in the incoming packet.
- MD5 digests differ on the router and in the incoming packet.
- Text authentication strings differ on the router and in the incoming packet.

- Configuring GLBP MD5 Authentication Using a Key String, page 11
- Configuring GLBP MD5 Authentication Using a Key Chain, page 13
- Configuring GLBP Text Authentication, page 15

Configuring GLBP MD5 Authentication Using a Key String

Configuring GLBP MD5 authentication protects the router against spoofing software and uses the industry-standard MD5 algorithm for improved reliability and security.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** *ipv6-address / prefix-length* | *prefix-name ipv6-prefix / prefix-length* | **autoconfig** [*default-route*]}
5. **glbp** *group-number* **authentication md5 key-string** [**0** | **7**] *key*
6. **glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**
7. Repeat Steps 1 through 6 on each router that will communicate.
8. **end**
9. **show glbp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0/1`	Configures an interface type and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address* / *prefix-length* | *prefix-name ipv6-prefix* / *prefix-length* | **autoconfig** [*default-route*]} **Example:** `Router(config-if)# ipv6 address 2001:DB8:0:7272::72/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 5	**glbp** *group-number* **authentication md5 key-string** [**0** | **7**] *key* **Example:** `Router(config-if)# glbp 1 authentication md5 key-string d00b4r987654321a`	Configures an authentication key for GLBP MD5 authentication. • The number of characters in the command plus the key string must not exceed 255 characters. • No keyword before the *key* argument or specifying **0** means the key is unencrypted. • Specifying **7** means the key is encrypted. The key-string authentication key will automatically be encrypted if the **service password-encryption** global configuration command is enabled.
Step 6	**glbp** *group* **ipv6** [*ipv6-address* | **autoconfig** **Example:** `Router(config-if)# glbp 1 ipv6 FE80::260:3EFF:FE11:6770`	Enables GLBP in IPv6.
Step 7	Repeat Steps 1 through 6 on each router that will communicate.	--
Step 8	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 9	**show glbp** **Example:** `Router# show glbp`	(Optional) Displays GLBP information. • Use this command to verify your configuration. The key string and authentication type will be displayed if configured.

Configuring GLBP MD5 Authentication Using a Key Chain

Key chains allow a different key string to be used at different times according to the key chain configuration. GLBP will query the appropriate key chain to obtain the current live key and key ID for the specified key chain.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. **key** *key-id*
5. **key-string** *string*
6. **exit**
7. **exit**
8. **interface** *type number*
9. **ipv6 address** *ipv6-address / prefix-length* | *prefix-name ipv6-prefix / prefix-length* | **autoconfig** [*default-route*]}
10. **glbp** *group-number* **authentication md5 key-chain** *name-of-chain*
11. **glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**
12. Repeat Steps 1 through 11 on each router that will communicate.
13. **end**
14. **show glbp**
15. **show key chain**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**key chain** *name-of-chain* **Example:** `Router(config)# key chain glbp2`	Enables authentication for routing protocols and identifies a group of authentication keys.
Step 4	**key** *key-id* **Example:** `Router(config-keychain)# key 100`	Identifies an authentication key on a key chain. • The *key-id* must be a number.
Step 5	**key-string** *string* **Example:** `Router(config-keychain-key)# key-string string1`	Specifies the authentication string for a key. • The *string* can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral.
Step 6	**exit** **Example:** `Router(config-keychain-key)# exit`	Returns to keychain configuration mode.
Step 7	**exit** **Example:** `Router(config-keychain)# exit`	Returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0/1`	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 9	**ipv6 address** *ipv6-address / prefix-length* | *prefix-name ipv6-prefix / prefix-length* | **autoconfig** [*default-route*]} **Example:** `Router(config-if)# ipv6 address 2001:DB8:0:7272::72/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 10	**glbp** *group-number* **authentication md5 key-chain** *name-of-chain* **Example:** `Router(config-if)# glbp 1 authentication md5 key-chain glbp2`	Configures an authentication MD5 key chain for GLBP MD5 authentication. • The key chain name must match the name specified in Step 3.
Step 11	**glbp** *group* **ipv6** [*ipv6-address* | **autoconfig** **Example:** `Router(config-if)# glbp 1 ipv6 FE80::E0:F727:E400:A`	Enables GLBP in IPv6.
Step 12	Repeat Steps 1 through 11 on each router that will communicate.	--
Step 13	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 14	**show glbp** **Example:** `Router# show glbp`	(Optional) Displays GLBP information. • Use this command to verify your configuration. The key chain and authentication type will be displayed if configured.
Step 15	**show key chain** **Example:** `Router# show key chain`	(Optional) Displays authentication key information.

Configuring GLBP Text Authentication

This method of authentication provides minimal security. Use MD5 authentication if security is required.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** *ipv6-address* / *prefix-length* | *prefix-name ipv6-prefix* / *prefix-length* | **autoconfig** [*default-route*]}
5. **glbp** *group-number* **authentication text** *string*
6. **glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**
7. Repeat Steps 1 through 6 on each router that will communicate.
8. **end**
9. **show glbp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface Ethernet 0/1`	Configures an interface type and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address* / *prefix-length* | *prefix-name ipv6-prefix* / *prefix-length* | **autoconfig** [*default-route*]} **Example:** `Router(config-if)# ipv6 address 2001:DB8:0:7272::72/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 5	**glbp** *group-number* **authentication text** *string* **Example:** `Router(config-if)# glbp 10 authentication text stringxyz`	Authenticates GLBP packets received from other routers in the group. • If you configure authentication, all routers within the GLBP group must use the same authentication string.

	Command or Action	Purpose
Step 6	**glbp** *group* **ipv6** [*ipv6-address* | **autoconfig** **Example:** `Router(config-if)# glbp 1 ipv6 FE80::60:3E47:AC8:8`	Enables GLBP in IPv6.
Step 7	Repeat Steps 1 through 6 on each router that will communicate.	--
Step 8	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 9	**show glbp** **Example:** `Router# show glbp`	(Optional) Displays GLBP information. • Use this command to verify your configuration.

Configuring GLBP Weighting Values and Object Tracking

GLBP weighting is used to determine whether a router can act as a virtual forwarder. Initial weighting values can be set and optional thresholds specified. Interface states can be tracked and a decrement value set to reduce the weighting value if the interface goes down. When the GLBP router weighting drops below a specified value, the router will no longer be an active virtual forwarder. When the weighting rises above a specified value, the router can resume its role as an active virtual forwarder.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **track** *object-number* **interface** *type number* {**line-protocol** | **ip routing**
4. **interface** *type number*
5. **glbp** *group* **weighting** *maximum* **lower** *lower*] [**upper** *upper*
6. **glbp** *group* **weighting track** *object-number* [**decrement** *value*]
7. **glbp** *group* **forwarder preempt** [**delay minimum** *seconds*]
8. **end**
9. **show track** [*object-number*| **brief**] [**interface** [**brief**]| **ip route** [**brief**] | **resolution**| **timers**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**track** *object-number* **interface** *type number* {**line-protocol** | **ip routing** **Example:** `Router(config)# track 2 interface POS 6/0 ip routing`	Configures an interface to be tracked where changes in the state of the interface affect the weighting of a GLBP gateway, and enters tracking configuration mode. • This command configures the interface and corresponding object number to be used with the **glbp weighting track** command. • The **line-protocol** keyword tracks whether the interface is up. The **ip routing** keywords also check that IPv6 routing is enabled on the interface and an IPv6 address is configured.
Step 4	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Enters interface configuration mode.
Step 5	**glbp** *group* **weighting** *maximum* **lower** *lower*] [**upper** *upper* **Example:** `Router(config-if)# glbp 10 weighting 110 lower 95 upper 105`	Specifies the initial weighting value, and the upper and lower thresholds, for a GLBP gateway.
Step 6	**glbp** *group* **weighting track** *object-number* [**decrement** *value*] **Example:** `Router(config-if)# glbp 10 weighting track 2 decrement 5`	Specifies an object to be tracked that affects the weighting of a GLBP gateway. • The *value* argument specifies a reduction in the weighting of a GLBP gateway when a tracked object fails.

	Command or Action	Purpose
Step 7	**glbp** *group* **forwarder preempt** [**delay minimum** *seconds*] **Example:** `Router(config-if)# glbp 10 forwarder preempt delay minimum 60`	Configures the router to take over as the AVF for a GLBP group if the current AVF for a GLBP group falls below its low weighting threshold. • This command is enabled by default with a delay of 30 seconds. • Use the optional **delay** and **minimum** keywords and the *seconds* argument to specify a minimum delay interval in seconds before preemption of the AVF takes place.
Step 8	**end** **Example:** `Router(config-if)# exit`	Returns to privileged EXEC mode.
Step 9	**show track** [*object-number*| **brief**] [**interface** [**brief**]| **ip route** [**brief**]	**resolution**| **timers**] **Example:** `Router# show track 2`	Displays tracking information.

Enabling and Verifying GLBP

GLBP is designed to be easy to configure. Each gateway in a GLBP group must be configured with the same group number, and at least one gateway in the GLBP group must be configured with the virtual IPv6 address to be used by the group. All other required parameters can be learned.

If VLANs are in use on an interface, the GLBP group number must be different for each VLAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 address** *ipv6-address* / *prefix-length* | *prefix-name ipv6-prefix* / *prefix-length* | **autoconfig** [*default-route*]}
5. **glbp** *group* **ipv6** [*ipv6-address* | **autoconfig**
6. **exit**
7. **show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 address** *ipv6-address* / *prefix-length* | *prefix-name ipv6-prefix* / *prefix-length* | **autoconfig** [*default-route*]} **Example:** `Router(config-if)# ipv6 address 2001:DB8:0:7262::62/64`	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
Step 5	**glbp** *group* **ipv6** [*ipv6-address* | **autoconfig** **Example:** `Router(config-if)# glbp 1 ipv6 FE80::60:3E47:AC8:8`	Enables GLBP in IPv6.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode, and returns the router to global configuration mode.
Step 7	**show glbp** [*interface-type interface-number*] [*group*] [*state*] [**brief**] **Example:** `Router(config)# show glbp 10`	(Optional) Displays information about GLBP groups on a router. • Use the optional **brief** keyword to display a single line of information about each virtual gateway or virtual forwarder.

Troubleshooting the GLBP

This task requires a router running GLBP to be attached directly to a console.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no logging console**
4. Use Telnet to access a router port and repeat Steps 1 and 2.
5. **end**
6. **terminal monitor**
7. **debug condition glbp** *interface-type interface-number group* [*forwarder*]
8. **terminal no monitor**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**no logging console** **Example:** `Router(config)#` **`no logging console`**	Disables all logging to the console terminal. • To reenable logging to the console, use the **logging console** command in global configuration mode.
Step 4	Use Telnet to access a router port and repeat Steps 1 and 2.	Enters global configuration mode in a recursive Telnet session, which allows the output to be redirected away from the console port.
Step 5	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 6	**terminal monitor** **Example:** `Router#` **terminal monitor**	Enables logging output on the virtual terminal.
Step 7	**debug condition glbp** *interface-type interface-number group* [*forwarder*] **Example:** `Router#` **debug condition glbp fastethernet 0/0 10 1**	Displays debugging messages about GLBP conditions. • Try to enter only specific **debug condition glbp**or **debug glbp**commands to isolate the output to a certain subcomponent and minimize the load on the processor. Use appropriate arguments and keywords to generate more detailed debug information on specified subcomponents. • Enter the specific **no debug condition glbp**or **no debug glbp** command when you are finished.
Step 8	**terminal no monitor** **Example:** `Router#` **terminal no monitor**	Disables logging on the virtual terminal.

Enabling an HSRP Group for IPv6 Operation

HSRP version 2 must be enabled on an interface before HSRP IPv6 can be configured.

- Enabling HSRP Version 2, page 22
- Enabling and Verifying an HSRP Group for IPv6 Operation, page 23

Enabling HSRP Version 2

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **standby version** {**1**| **2**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.
Step 4	**standby version** {**1**| **2** **Example:** `Router(config-if)# standby version 2`	Changes the version of the HSRP. • Version 1 is the default.

Enabling and Verifying an HSRP Group for IPv6 Operation

In this task, when you enter the **standby ipv6** command, a modified EUI-64 format interface identifier is generated in which the EUI-64 interface identifier is created from the relevant HSRP virtual MAC address.

In IPv6, a router on the link advertises in RA messages any site-local and global prefixes, and its willingness to function as a default router for the link. RA messages are sent periodically and in response to router solicitation messages, which are sent by hosts at system startup.

A node on the link can automatically configure site-local and global IPv6 addresses by appending its interface identifier (64 bits) to the prefixes (64 bits) included in the RA messages. The resulting 128-bit IPv6 addresses configured by the node are then subjected to duplicate address detection to ensure their uniqueness on the link. If the prefixes advertised in the RA messages are globally unique, then the IPv6 addresses configured by the node are also guaranteed to be globally unique. Router solicitation messages, which have a value of 133 in the Type field of the ICMPv6 packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **interface** *type number*
5. **standby** [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address* / *prefix-length* | *ipv6-prefix* / *prefix-length* | *link-local-address* | **autoconfig**
6. **standby** [*group-number*] **preempt** [**delay minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}]
7. **standby** [*group-number*] **priority** *priority*
8. **exit**
9. **show standby** [*type number* [*group*]] [**all** | **brief**
10. **show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 unicast-routing** **Example:** `Router(config)# ipv6 unicast-routing`	Enables the forwarding of IPv6 unicast datagrams. • The **ipv6 unicast-routing** command must be enabled for HSRP for IPv6 to work.
Step 4	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies an interface type and number, and places the router in interface configuration mode.

	Command or Action	Purpose
Step 5	**standby** [*group-number*] **ipv6** {*ipv6-global-address* | *ipv6-address* / *prefix-length* | *ipv6-prefix* / *prefix-length* | *link-local-address* | **autoconfig** **Example:** `Router(config-if)# standby 1 ipv6 autoconfig`	Activates the HSRP in IPv6. If an IPv6 address is used, it must include an IPv6 prefix length. If a link-local address is used, it must not have a prefix.
Step 6	**standby** [*group-number*] **preempt** [**delay minimum** *seconds* | **reload** *seconds* | **sync** *seconds*}] **Example:** `Router(config-if)# standby 1 preempt`	Configures HSRP preemption and preemption delay.
Step 7	**standby** [*group-number*] **priority** *priority* **Example:** `Router(config-if)# standby 1 priority 110`	Configures HSRP priority.
Step 8	**exit** **Example:** `Router(config-if)# exit`	Returns the router to privileged EXEC mode.
Step 9	**show standby** [*type number* [*group*]] [**all** | **brief** **Example:** `Router# show standby`	Displays HSRP information.
Step 10	**show ipv6 interface** [**brief**] [*interface-type interface-number*] [**prefix** **Example:** `Router# show ipv6 interface ethernet 0/0`	Displays the usability status of interfaces configured for IPv6.

Configuration Examples for First Hop Redundancy Protocols in IPv6

Example Customizing GLBP Configuration

In the following example, Router A, shown in Figure 1, is configured with a number of GLBP commands:

```
interface fastethernet 0/0
 ipv6 address 2001:DB8:0001:0001:/64
 glbp 10 timers 5 18
 glbp 10 timers redirect 600 7200
 glbp 10 load-balancing host-dependent
 glbp 10 priority 254
 glbp 10 preempt delay minimum 60
```

Example GLBP MD5 Authentication Using Key Strings

The following example configures GLBP MD5 authentication using a key string:

```
!
interface Ethernet 0/1
 ipv6 address 2001:DB8:0001:0001:/64
 glbp 2 authentication md5 key-string ThisStringIsTheSecretKey
 glbp 2 ipv6 FE80::260:3EFF:FE11:6770
```

Example GLBP MD5 Authentication Using Key Chains

In the following example, GLBP queries the key chain "AuthenticateGLBP" to obtain the current live key and key ID for the specified key chain:

```
key chain AuthenticateGLBP
 key 1
  key-string ThisIsASecretKey
interface Ethernet 0/1
 ipv6 address 2001:DB8:0001:0001:/64
 glbp 2 authentication md5 key-chain AuthenticateGLBP
 glbp 2 ipv6 FE80::E0:F727:E400:A
```

Example GLBP Text Authentication

The following example configures GLBP text authentication using a text string:

```
interface fastethernet 0/0
 ipv6 address 2001:DB8:0001:0001:/64
 glbp 10 authentication text stringxyz
 glbp 10 ipv6 FE80::60:3E47:AC8:8
```

Example GLBP Weighting

In the following example, Router A, shown in Figure 1, is configured to track the IP routing state of the POS interfaces 5/0 and 6/0, an initial GLBP weighting with upper and lower thresholds is set, and a

weighting decrement value of 10 is set. If POS interfaces 5/0 and 6/0 go down, the weighting value of the router is reduced.

```
track 1 interface POS 5/0 ip routing
track 2 interface POS 6/0 ip routing
interface fastethernet 0/0
 glbp 10 weighting 110 lower 95 upper 105
 glbp 10 weighting track 1 decrement 10
 glbp 10 weighting track 2 decrement 10
 glbp 10 forwarder preempt delay minimum 60
```

Example Enabling GLBP Configuration

In the following example, the router is configured to enable GLBP, and the virtual IPv6 address of 2001:DB8:0002:0002:/64 is specified for GLBP group 10:

```
interface fastethernet 0/0
ipv6 address 2001:DB8:0001:0001:/64
 glbp 10 ipv6 FE80::60:3E47:AC8:8
```

In the following example, GLBP for IPv6 is enabled for GLBP group 15:

```
interface fastethernet 0/0
 ipv6 address 2001:DB8:0001:0001:/64
 glbp 10 ipv6
```

Example Enabling and Verifying an HSRP Group for IPv6 Operation

- Example Configuration and Verification for an HSRP Group, page 27
- Example Configuring HSRP Global IPv6 Addresses, page 28

Example Configuration and Verification for an HSRP Group

The following example shows configuration and verification for an HSRP group for IPv6 that consists of Router1 and Router2. The **show standby** command is issued for each router to verify the router's configuration.

Router 1 Configuration

```
interface FastEthernet0/0.100
description DATA VLAN for PCs
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1010/64
standby version 2
standby 101 priority 120
standby 101 preempt delay minimum 30
standby 101 authentication ese
standby 101 track Serial0/1/0.17 90
standby 201 ipv6 autoconfig
standby 201 priority 120
standby 201 preempt delay minimum 30
standby 201 authentication ese
standby 201 track Serial0/1/0.17 90
Router1# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Active
2 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
```

```
Next hello sent in 2.296 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Active
2 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 2.428 secs
Authentication text "ese"
Preemption enabled, delay min 30 secs
Active router is local
Standby router is FE80::20F:8FFF:FE37:3B70, priority 100 (expires in 7.856 sec)
Priority 120 (configured 120)
Track interface Serial0/1/0.17 state Up decrement 90
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

Router 2 Configuration

```
interface FastEthernet0/0.100
description DATA VLAN for Computers
encapsulation dot1Q 100
ipv6 address 2001:DB8:CAFE:2100::BAD1:1020/64
standby version 2
standby 101 preempt
standby 101 authentication ese
standby 201 ipv6 autoconfig
standby 201 preempt
standby 201 authentication ese
Router2# show standby
FastEthernet0/0.100 - Group 101 (version 2)
State is Standby
7 state changes, last state change 5w5d
Active virtual MAC address is 0000.0c9f.f065
Local virtual MAC address is 0000.0c9f.f065 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-101" (default)
FastEthernet0/0.100 - Group 201 (version 2)
State is Standby
7 state changes, last state change 5w5d
Virtual IP address is FE80::5:73FF:FEA0:C9
Active virtual MAC address is 0005.73a0.00c9
Local virtual MAC address is 0005.73a0.00c9 (v2 IPv6 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.936 secs
Authentication text "ese"
Preemption enabled
Active router is FE80::212:7FFF:FEC6:8F0C, priority 120 (expires in 7.548 sec)
MAC address is 0012.7fc6.8f0c
Standby router is local
Priority 100 (default 100)
IP redundancy name is "hsrp-Fa0/0.100-201" (default)
```

Example Configuring HSRP Global IPv6 Addresses

The following example shows three HSRP global IPv6 addresses with an explicitly configured link-local address:

```
interface Ethernet0/0
 no ip address
 ipv6 address 2001::DB8:1/64
 standby version 2
 standby 1 ipv6 FE80::1:CAFÉ
 standby 1 ipv6 2001::DB8:2/64
 standby 1 ipv6 2001:DB8::3/64
 standby 1 ipv6 2001:DB8::4/64
end
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 link-local addresses and stateless autoconfiguration	" Implementing IPv6 Addressing and Basic Connectivity ," *Cisco IOS IPv6 Configuration Guide*
IPv6 commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IPv6 Command Reference*
Configuring HSRP in IPv4	" Configuring HSRP ," *Cisco IOS IP Application Services Configuration Guide*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2281	*Cisco Hot Standby Router Protocol (HSRP)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for First Hop Redundancy Protocols in IPv6

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for First Hop Redundancy Protocols for IPv6

Feature Name	Releases	Feature Configuration Information
FHRP--GLBP Support for IPv6	12.2(58)SE 12.2(33)SXI 12.4(6)T	GLBP protects data traffic from a failed router or circuit while allowing packet load sharing between a group of redundant routers. The following commands were introduced or modified for this feature: **glbp forwarder preempt**, **glbp ipv6**, **glbp load-balancing**, **glbp preempt**, **glbp priority**, **glbp name**, **glbp timers**, **glbp timers redirect**, **glbp weighting**, **glbp weighting track**, **track interface**.

Feature Name	Releases	Feature Configuration Information
GLBP MD5 Authentication	12.2(18)S 12.3(2)T	MD5 authentication provides greater security than the alternative plain text authentication scheme. MD5 authentication allows each GLBP group member to use a secret key to generate a keyed MD5 hash that is part of the outgoing packet. A keyed hash of an incoming packet is generated and, if the hash within the incoming packet does not match the generated hash, the packet is ignored. The following commands were introduced or modified for this feature: **glbp authentication**, **key**, **key chain**, **key-string (authentication)**, **show glbp**, **show key chain**.
IPv6 Services--HSRP for IPv6	12.4(4)T 12.2(33)SRB 12.2(33)SXI	The HSRP is an FHRP designed to allow for transparent failover of the first-hop IPv6 router. The following commands were introduced or modified by this feature: **show standby**, standby ipv6, standby preempt, standby priority.
HSRP--Global IPv6 Addresses	12.2(33)SXI4 15.0(1)SY	The HSRP global IPv6 address feature allows users to configure multiple non-link local addresses as virtual addresses. The following command was modified by this feature: standby ipv6.

Glossary

- **CPE** --Customer premises equipment
- **FHRP** --First hop redundancy protocol
- **GLBP** --Gateway load balancing protocol
- **HSRP** --Hot standby routing protocol
- **NA** --Neighbor advertisement
- **ND** --Neighbor Discovery
- **NS** --Neighbor solicitation
- **PE** --Provider equipment
- **RA** --Router advertisement
- **RS** --Router solicitation